REMARKS

Claims 1-16 are pending. By this response, claims 1 and 9 are amended. Claims 6 and 14-16 have been indicated as containing allowable subject matter. Reconsideration and allowance based on the above amendments and the following remarks are respectfully requested.

The Office Action rejections claim 1-3, 5 and 9-12 under 35 U.S.C. § 103(e) as being anticipated by Sheymov et al. (U.S. 2002/0023227) and claims 4, 5, 7, 8, 12, 13 and 17 under 35 U.S.C. § 103(a) as being unpatentable over Sheymov and Osborne et al. (U.S. 6,687,833). These rejections are respectfully traversed.

Each of independent claims 1, 9 and 13 refer to the preparation of a response to an illegal access by a communication device on an internal network server. For example, Fig. 4 illustrates that a packet P4, which is a response packet prepared by the decoy server, has the same address as that of target server to be attacked. The preparation of the response is performed by a decoy server or data center remotely located from the internal network over the internet. The decoy server or data center encapsulates the response and sends it to the internal network to perform decapulation and to send the response to the communication device.

In the embodiments of claims 1, 9 and 13 the entire response is developed by the decoy server or data center and the origin information of the response has already been removed. Thus, in order to send the response to the internal network, encapsulation becomes necessary.

In contrast, Sheymov teaches a system in which an intrusion detection system 110 sends intrusion information to a monitoring system by way of an analysis system 120 and network 10. The monitoring 140 provides instructions to the analysis system 120 and intrusion detection system 110 for engaging the hacker. The analysis system develops a response from the provided

information and therefore must also include the decoy origin information of the response to the hacker. See paragraph 46 and 47.

Therefore, Sheymov monitoring center, which the Office Action alleges is Applicants' claimed decoy server and data center, does not prepare a response with the origination information as in the claims of the present invention. In Sheymov this is prepared and attached by the analysis system an intrusion detection not by the monitoring center 140.

Further, Sheymov does not teach encapsulation and decapsulation of a data sent from the decoy server to the internal network. Encapsulation is necessary since the data sent from the decoy service has the origin information already stripped off and a decoy origin information (same as the information of the target server) added thereto. This is not necessary in Sheymov because the decoy original information is not added until the response is prepared at the analysis system and information detection system.

Osborne is provided to teach the encapsulation and decapsulation of data. Applicants submit that encapsulation and decapsulation by themselves are not novel, but used in certain context could be novel. The specific features of Applicants' claims utilize encapsulation and decapsulation because of the specific manner in which response data sent to a hacker is created. In Sheymov encapsulation is unnecessary, as discussed above. Therefore, one of ordinary skill would not look to Osborne's teachings of encapsulation and decapsulation and provide these features with the system of Sheymov as they would serve no purpose in Sheymov's system.

Therefore, Sheymov alone or in combination with Osborne fail to teach or suggest, *inter alia*, a decoy server functionally coupled to the control system, wherein the apparatus is placed outside an internal communication network, for receiving illegal access data transmitted from a

data communication device placed outside the internal communication network for a purpose of illegally accessing the internal communication network, therefore taking countermeasures against the illegal access data received, furthermore the countermeasures include providing a response returning to originate from the internal communication network, the response being encapsulated and sent to a network device within the given internal communication network to be decapsulated and transmitted by the network device to the data communication device, as recited in claim 1.

Sheymov and Osborne fail to teach, *inter alia*, taking internal measures against the illegal access data received by a data center remotely located from the internet from the internal network, and the countermeasures include providing a response pretending to originate from the internal communication network, response being encapsulated by the data center and sent to a network device within the internal communication network to be decapsulated and transmitted by the network device to the communication device, as recited in claim 9.

Also, Sheymov and Osborne fail to teach, *inter alia*, receiving an encapsulated unauthorized access packet at a data center placed outside the internal network ... analyzing the received packet to form a response packet; encapsulating the response packet so that it appears to originate from a target server; sending the encapsulating response packet to a network device, wherein the network device is within the internal network and wherein the network device decapsulates the encapsulated response packet and forwards the decapsulated packet to the source of the unauthorized access packet, as recited in claim 13.

In view of the above, Applicants respectfully submit that Sheymov along with the combination of Osborne fail to teach each and every feature of Applicants' independent claims 1,

9 and 13. Dependent claims are also distinguishable from the cited references for the above reasons as well as for the additional features they recite. Accordingly, reconsideration and withdrawal of the rejection are respectfully requested.

CONCLUSION

For at least these reasons, it is respectfully submitted that claims 1-16 are distinguishable over the cited art. Favorable consideration and prompt allowance are earnestly solicited.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Chad J. Billings Reg. No. 48,917 at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37.C.F.R. §§1.16 or 1.14; particularly, extension of time fees.

Dated: February 27, 2007

Respectfully submitted,

By C. Billings 48,917
for D. Richard Anderson
Registration No.: 40,439
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant